REMARKS

Reconsideration of the rejections set forth in the Office Action dated October 7, 2008, is respectfully requested. In the Office Action, the Examiner rejected claims 54-74. Applicant has amended claims 54, 65, and 74. Accordingly, claims 54-74 are pending in the application, and no new matter has been added as can be confirmed by the Examiner.

A. The Cited Prior Art References Do Not Disclose or Suggest the Combination of Authenticating a Request for Data Content from a Computer System by Comparing a Computer Identification Code with Computer Identification Data, Wherein the Computer Identification Code Uniquely Identifies a Selectively Chosen Computer System and the Computer Identification Data Includes Current Information for Identifying the Computer System That Activated the Hyperlink, as Recited in Claims 54-74.

In the Office Action, the Examiner rejected claims 54-74 each under 35 U.S.C. § 103(a) as allegedly being rendered obvious by Bezos et al., United States Patent No. 6,029,141, in view of Messer et al., United States Application Publication No. 2004/0230491, in further view of Dane et al., United States Application Publication No. 2004/0215623. Applicant respectfully submits, however, that at least one recited element of independent claims 54, 65, and 74, is totally missing from the cited prior art references, both individually and in combination. Accordingly, claims 54-74 are in condition for allowance.

According to the Examiner, Bezos et al. disclose identifying the user computer and comparing the user computer identification to other computer identifying information to determine which computer this is and whether it is a known or new computer. Examiner references Bezos et al. disclosure of the utilization of "cookie" technology in the identification of a user for the merchant in creating or retrieving existing electronic shopping carts. As cited by the Examiner, Bezos et al. teach:

> Because the identity of the customer is normally unknown to the merchant Web site 106 at the time of the referral event, the site 106 uses cookies technology to identify the customer, so that the **customer can be associated with an existing shopping cart created during previous visits** to the site 106.... If **no shopping cart exists for the customer**, or if no cookie exists on the customer computer 108, **a shopping cart structure is created** for the user. (col 8, lines 15-28).

As Bezos et al. disclose,"The shopping cart is a customer-specific data structure that is generated and maintained by executable code of the merchant site." (col 7, lines 61-63).

Examiner also asserts that though Bezos et al. do not explicitly disclose that the original referral link can include the unique customer ID before selection, Bezos et al. do disclose that the unique customer ID can be generated or added to the URL upon the user selecting a referral link, that the unique user ID can be made part of the advertising content that is presented to the user as the user shops, and that the unique customer ID can be part of the URL for subsequent activity even if the user remains on the original advertiser webpage (col 13, line 40—col 14, line 10). Examiner argues that changing the sequence from including the unique customer ID before selection to after selection is intrinsically obvious.

In contrast, independent claims 54, 65, and 74 each recite the combination of authenticating a request for data content, received from a computer system, by "comparing the computer identification code with the computer identification data," wherein "the computer identification code uniquely identif[ies] a selectively chosen computer system" and "the computer identification data includ[es] current information for identifying the computer system that activated the hyperlink." Applicant's Specification teaches:

> Unlike more traditional advertising modalities, advertising on ... the Internet does not readily provide the type of information upon which to base a fee for advertising between a merchant and advertiser. ...One attempt to solve this apparent value for service problem is to pay the advertiser **based on the number of 'clicks' on the advertisement**... Probably the most egregious problem is that of advertiser **fraud through the generation of fraudulent clicks**. ...[A] fee per click/activity payment method provides a greater incentive to the advertiser to place the advertisement in front of as many consumers as possible, regardless of the consumer's market profile. ...The clicking by the user on the advertisement or link causes the count of the clicks, that is, the number of responses, for the advertisement to be increased as the counter does not, and cannot, differentiate as to the manner in which the request to view the full advertisement is made, for example, through an email or on a web site page. ...[I]t is problematic in that most of the audience of the advertising link is **not a target audience**. Thus, the merchant will, most likely, pay disproportionate advertising costs in relationship to the number of sales. (Specification, paragraphs [0005] – [0010]).

In addressing the above, and other issues, as set forth in claims 54, 65, and 74, authenticating a

request for data content is performed by comparing the computer identification code and the computer identification data. The computer identification code of claims 54, 65, and 74 is dynamically generated upon initialization of the hyperlink on the selectively chosen computer system, whereas the computer identification data includes current information for identifying a computer system that activated the hyperlink. Therefore, independent claims 54, 65, and 74 do not include utilizing cookie technology to determine whether to associate a computer system to an existing shopping cart or whether to create a shopping cart as taught by Bezos et al.

Further, independent claims 54, 65, and 74 require computer identification code to be generated before selection of a referral link for authentication by comparison with computer identification data. By requiring the selection of a referral link before creating a "customer ID," Bezos et al. teach away from the authentication by comparison of computer identification code and the computer identification data as cited in independent claims 54, 65, and 74. Therefore Bezos et al. do not bear upon the patentability of the claims 54, 65, and 74.

According to the Examiner, Messer et al. disclose determining invalid requests for information and tracking invalid requests for information, and utilizing a database and reporting for invalid requests for information. Messer et al. disclose a system by which an affiliate of a merchant allocates a banner advertisement block on a web page for presenting advertising material, such as a banner ad, for presentation via a user workstation. (See Messer et al. at [0024]) The banner ad is linked to a clearinghouse server and then to the merchant server. (See id. at [0025]). Messer et al. state that the linking allows for determining if and when a user utilizes the banner in a purchase from the merchant, and if to allocate a purchase commission to the affiliate. (See id.). As admitted by Examiner, Messer et al. discloses, "[0038] In addition to the Javascript detection algorithm, the system further tracks potential click fraud by assessing historical patterns of commerce. For example, if a click-through includes the same ID, the system measures the interval between successive clicks. A relatively fast click speed, or multiple clicks at a uniform interval reflects the possibility that the click is machine generated and potentially fraudulent. Other patters may give further details, such as large jumps in traffic from individual sites."

In contrast, independent claims 54, 65, and 74 each recite the combination of authenticating a request for data content, received from a computer system, by "comparing the computer identification code with the computer identification data," wherein "the computer identification code uniquely identif[ies] a selectively chosen computer system " and "the computer identification data includ[es] current information for identifying the computer system that activated the hyperlink." As set forth in claims 54, 65, and 74, authenticating a request for data content is performed by comparing the computer identification code and the computer identification data. The computer identification code of claims 54, 65, and 74 is dynamically generated upon initialization of the hyperlink on the selectively chosen computer system, whereas the computer identification data includes current information for identifying a computer system that activated the hyperlink. Therefore the authenticating of the request does not include assessing historical patterns of commerce or consideration of time intervals between successful clicks, as taught by Messer et al. Therefore Messer does not bear upon the patentability of the claims 54, 65, and 74.

Examiner relies on Dane et al. as disclosing that if a URL is found to be fraudulent then the system will record as much information as is available about the attempted fraudulent access to identify an individual or individuals who is attempting to improperly access the data. Examiner further asserts that Dane et al. discloses that, because the access has been determined to be fraudulent, the URL would be directed to a message indicating that access has been denied. Dane et al. discloses a resume database system which allows for resume records on the system to be viewed by others via URL. Further, it discloses the ability to add input from an unauthorized, but verified, user. Examiner does not assert that Dane et al. teaches the combination of authenticating a request for data content, received from a computer system, by "comparing the computer identification code with the computer identification data," wherein "the computer identification code uniquely identif[ies] the computer system" and "the computer identification data includ[es] current information for identifying the computer system." Therefore Dane et al. does not bear upon the patentability of claims 54, 65, and 74.

The Examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. In view of all factual information, the examiner must then make a determination whether the claimed invention "as a whole" would have been obvious at that time to that person. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art. (M.P.E.P. § 2142).

Here, the Examiner has not established a *prima facie* case under 35 U.S.C. § 103(a) because, as shown above, all of the elements of the pending claims are not found in the cited references. None of the above references, neither individually nor in combination, disclose or even suggest authenticating a request for data content from a computer system by comparing the computer identification code with the computer identification data, wherein the computer identification code uniquely identifies the computer system and the computer identification data includes current information for identifying the computer system. Accordingly, at least one recited element of claims 54, 65, and 74 is totally missing from the cited prior art references. Applicant therefore submits that claims 54, 65, and 74 are not anticipated or rendered obvious by Bezos et al., Messer et al., or Dane et al. and that claims 54-74 are in condition for allowance.

Accordingly, for at least the reasons set forth above, it is submitted that claims 54-74 are in condition for allowance. A Notice of Allowance is earnestly solicited. The Examiner is encouraged to contact the undersigned at (949) 567-6700 if there is any way to expedite the prosecution of the present application.

Respectfully submitted,

Dated: April 7, 2009

By: _____
Osama Hussain
Reg. No. 54,591
Attorneys for Applicant

Osama Hussain
BayTSP
P.O. Box 1314
Los Gatos, CA 95031
Telephone: (408) 341-2345
Facsimile: (408) 376-2005